No. 15-2560

UNITED STATES COURT OF APPEALS
FOR THE FOURTH CIRCUIT

WIKIMEDIA FOUNDATION, *et al.*,

Plaintiffs–Appellants,

v.

NATIONAL SECURITY AGENCY, *et al.*,

Defendants–Appellees.

On Appeal from the United States District Court
for the District of Maryland
Baltimore Division

REPLY BRIEF FOR PLAINTIFFS–APPELLANTS

Patrick Toomey
Jameel Jaffer
Alexander Abdo
Ashley Gorski
Brett Max Kaufman
AMERICAN CIVIL LIBERTIES UNION FOUNDATION
125 Broad Street, 18th Floor
New York, NY 10004
Phone: (212) 549-2500
ptoomey@aclu.org

Deborah A. Jeon
David R. Rocah
AMERICAN CIVIL LIBERTIES UNION FOUNDATION OF MARYLAND
3600 Clipper Mill Rd., #350
Baltimore, MD 21211
Phone: (410) 889-8555
jeon@aclu-md.org

Counsel for Plaintiffs–Appellants
(additional counsel on reverse)

Charles S. Sims
David A. Munkittrick
Proskauer Rose LLP
Eleven Times Square
New York, NY 10036
Phone: (212) 969-3000
csims@proskauer.com

Counsel for Plaintiffs–Appellants

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Rules

Other Authorities

INTRODUCTION

Plaintiffs challenge a government surveillance program that is unprecedented in its scope—a program that intrudes on the privacy of their internet communications and impairs their expressive and associational rights. The challenged surveillance, known as Upstream surveillance, involves the suspicionless seizure and searching of Americans' internet communications as they enter and leave the United States. The government has acknowledged that it is engaged in this surveillance and that the surveillance involves searching the communications of individuals who are neither foreign-intelligence targets nor in contact with those targets. As Plaintiffs have explained, what the government is doing here is the digital equivalent of searching the contents of every letter passing through major mail processing centers to identify those that mention certain information of interest.

Plaintiffs have plausibly alleged that their communications are being seized and searched in the course of this surveillance. First, Plaintiff Wikimedia has plausibly alleged that the government is copying and reviewing at least some of its trillion or more annual communications. Indeed, the allegation is more than plausible because the government has acknowledged that it is conducting Upstream surveillance on multiple major internet circuits, and as the Amended Complaint makes clear: (1) Wikimedia communicates with hundreds of millions of

people around the world, and those communications traverse every major internet circuit entering or leaving the United States; and (2) as a technological matter, Upstream surveillance requires that the NSA copy and review all international text-based communications transiting the circuits it is monitoring.

Separately, each of the Plaintiffs has plausibly alleged that the NSA is copying and reviewing substantially all text-based communications entering and leaving the United States. This conclusion follows necessarily from the government's own description of Upstream surveillance and from basic facts about the routing of communications across the internet backbone.

The government attacks the plausibility of Plaintiffs' detailed allegations, but it reaches its desired result only by disregarding all three of the procedural rules that apply on a motion like this one: the presumption of truth that attaches to Plaintiffs' factual allegations; the rule that all reasonable inferences are to be drawn in Plaintiffs' favor; and the rule that confines a plausibility challenge to the face of the pleadings. Indeed, in the end, the government resorts to outside declarations that the district court properly concluded must be disregarded at this stage of the case.

Plaintiffs have more than plausibly alleged the copying and review of their communications. Accordingly, this Court should reverse the district court's

dismissal of Plaintiffs' Amended Complaint and remand the case for further proceedings on the merits.

ARGUMENT

I. Plaintiffs have plausibly alleged the copying and review of their communications.

A. The government challenges the plausibility of the complaint, but it ignores the pleading standards.

The government urges the Court to apply a set of pleading standards that bear no resemblance to those governing a motion to dismiss.

First, although the government acknowledges that the Court must accept Plaintiffs' factual allegations as true, Def. Br. 25 (citing *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009)), in reality it asks the Court to do the opposite. It asks the Court to reject as "speculation" a series of detailed allegations grounded in (1) the myriad public disclosures concerning Upstream surveillance, and (2) provable facts about how the internet works. But nothing in *Iqbal*—or in *Amnesty*, for that matter—allows a court to dismiss as speculation the type of detailed, factual allegations that Plaintiffs have presented here. Of course, on a motion to dismiss, a court may disregard legal conclusions that are not supported by any facts. *See Iqbal*, 556 U.S. at 678. However, well-pled factual allegations that serve as the building blocks of a complaint must be credited as true. *See Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 555-57 (2007); *McLean v. United States*, 566 F.3d 391, 399 (4th Cir. 2009)

(refusing to "countenance . . . dismissals based on a judge's disbelief of a complaint's factual allegations"). In addition, in assessing whether a plaintiff's well-pled allegations together state a plausible claim on the face of the complaint, a court must draw all reasonable inferences in the plaintiff's favor. *See Wright v. North Carolina*, 787 F.3d 256, 263, 265 (4th Cir. 2015).[1]

Here, the government's insistence that Plaintiffs are simply speculating—when they describe the manner in which communications are routed across the internet and the scope of Upstream surveillance—is directly at odds with the legal standard on a motion to dismiss. The truth of these well-pled factual allegations, and the reasonable inferences that flow from them, is the starting-point for the Court's plausibility analysis.

Second, the government contends incorrectly that the Amended Complaint must be dismissed unless Plaintiffs prove from the outset that the copying and review of their communications is "certainly impending." Def. Br. 26-29. As an initial matter, Plaintiffs *have* alleged that their injuries are "certainly impending." Each Plaintiff has put forward a detailed claim that the NSA is presently copying and reviewing its communications in the course of Upstream surveillance. *See*

[1] The government also ignores the fact that the Court's plausibility analysis is limited to the pleadings and those documents incorporated by reference. Plaintiffs address this requirement below in explaining why the government's declarations are not properly before the Court. *See infra* Section I.D.

infra Section I.B-C. In any event, the government mischaracterizes the standards. As the Supreme Court recognized in *Amnesty*, and as it has reiterated since then, a plaintiff asserting future injuries need only show a "substantial risk" of harm. *Susan B. Anthony List v. Driehaus*, 134 S. Ct. 2334, 2341 (2014) (quoting *Clapper v. Amnesty Int'l USA*, 133 S. Ct. 1138, 1150 n.5 (2013)). Moreover, while a plaintiff must provide sufficient factual detail at the pleading stage to render its claim of standing "plausible," it is well-settled that a plaintiff need not plead every piece of evidence nor prove standing to a factual certainty. *See Lucas v. S. Carolina Coastal Council*, 505 U.S. 1003, 1012 n.3 (1992) (holding that even "a generalized allegation of injury in fact" suffices "at the pleading stage"); *Gwaltney of Smithfield, Ltd. v. Chesapeake Bay Found., Inc.*, 484 U.S. 49, 65-66 (1987); *see also* Br. of Law Professors 7-9, 12-14, ECF No. 32-1.[2] Standing, like the other elements of a claim, must be established "with the manner and degree of evidence required" at each "successive stage[] of the litigation." *Susan B. Anthony List*, 134 S. Ct. at 2342 (internal quotation marks omitted). The question at this stage of this

[2] The Supreme Court recognized this principle in *Amnesty* itself, distinguishing what must be pled from what must be proven at summary judgment. 133 S. Ct. at 1148-49 ("[A]t the summary judgment stage," a plaintiff "can no longer rest on . . . mere allegations, but must set forth by affidavit or other evidence specific facts.").

case is simply whether Plaintiffs' injuries, as set out in the Amended Complaint, are plausible. They surely are.[3]

B. Wikimedia has plausibly alleged the copying and review of its communications.

The Amended Complaint plausibly alleges, on the basis of the government's official disclosures and necessary inferences from those disclosures, that the NSA is copying and reviewing at least some of Wikimedia's trillion-plus international communications. Critically, the government has acknowledged that it is examining the contents of Americans' internet communications as they enter and leave the United States, in search of references to its tens of thousands of targets. *See* PCLOB Report 121-22, 113; *[Redacted]*, No. [Redacted], 2011 WL 10945618, at *15 (FISC Oct. 3, 2011). And it has acknowledged that it is conducting Upstream surveillance on multiple major internet circuits. *See* Pl. Br. 26. While the underlying technology may be complex, Wikimedia's two basic allegations are straightforward: (1) Wikimedia's communications traverse every major internet

[3] The government also argues that a heightened pleading standard applies because this case requires a court "to decide whether an action taken by one of the other two branches of the Federal Government was unconstitutional." Def. Br. 28 (quoting *Amnesty*, 133 S. Ct. at 1147). But Plaintiffs' claims also include a *statutory* challenge. Compl. ¶ 165 (JA 84). If the Court agrees with Plaintiffs that Section 702 authorizes the NSA to seize and search only the communications of individual targets—rather than those of everyone—then it need not reach Plaintiffs' constitutional claims. *See ACLU v. Clapper*, 785 F.3d 787, 792 (2d Cir. 2015).

circuit carrying traffic in and out of the United States; and (2) the government is copying and reviewing all of the international text-based communications on each of the circuits it monitors. Pl. Br. 24-39. These specific, factual allegations must be accepted as true, and together they plausibly plead the copying and review of Wikimedia's internet communications.

The government's arguments to the contrary are meritless.

First, the government says that Wikimedia "provide[s] no support" for the allegation that its communications traverse every major internet circuit carrying traffic in and out of the United States. Def. Br. 41. But this is not true. The Amended Complaint explains that Wikimedia communicates with hundreds of millions of individuals located in virtually every country on earth, and that its trillion-plus communications each year are routed across the limited number of major internet circuits that link the United States with the rest of the world. Pl. Br. 24-27; Compl. ¶¶ 60-62, 85, 88 (JA 47-48, 55-56). The government simply ignores these allegations. In reality, the government is arguing that Wikimedia has not supplied *proof*—at the pleading stage—of the truth of its allegations, but this argument only highlights the government's distortion of the pleading standards.

Second, the government also argues that the Court should not credit Plaintiffs' detailed allegation that the NSA is copying and reviewing all of the international text-based communications on each of the circuits it monitors.

Specifically, the government says that it has not "confirmed" the truth of this allegation. Def. Br. 42. But the government is wrong to suggest that the only allegations that count are the ones the government has expressly admitted to be true. *See Turkmen v. Hasty*, 789 F.3d 218, 242 (2d Cir. 2015). Just as importantly, Wikimedia has explained—in copious detail—why its allegations follow directly from the government's official acknowledgements about Upstream surveillance. Pl. Br. 27-33; Compl. ¶¶ 62-64 (JA 44, 48-49).[4] In short, the government *has* acknowledged it is systematically searching the *contents* of international communications for references to the NSA's tens of thousands of targets—what the PCLOB and the FISC call "about" surveillance. PCLOB Report 7, 37-39, 41 n.157. And, because of the way the internet works, the government could not conduct this type of surveillance except by copying and reviewing all of the international text-based communications on a given circuit. Pl. Br. 27-33.

[4] The government suggests that virtually nothing is publicly known about the scope and operation of Upstream surveillance, Def. Br. 23, 29, but that is inaccurate. The disclosures are extensive. The PCLOB described and analyzed Upstream in detail precisely because the surveillance relies on capabilities never before available to the government. *See, e.g.*, PCLOB Report 121-22; *id*. at 7-10, 12-13, 22, 30-41, 79. This report alone contains "over one hundred" newly declassified facts concerning Section 702 surveillance. PCLOB, Tr. of Public Meeting 8 (July 2, 2014), http://bit.ly/1SDbjcw. That is in addition to the many public sources—including FISC opinions, transparency reports, and public hearing testimony—cited in the report's hundreds of footnotes.

Relatedly, the government argues that "plaintiffs have provided no factual allegations to support" the scientific and technological principles that inform this allegation. Def. Br. 35, 39. But the Amended Complaint is replete with precisely these allegations, which explain in detail how communications are routed across the internet backbone and why Upstream surveillance entails the copying and review of all international text-based communications transiting the circuits the NSA is monitoring. Compl. ¶¶ 42, 44-45, 50, 62-64 (JA 41-42, 44, 48-49). Plaintiffs are prepared to prove their allegations on the merits, but they are not required to do so to survive a motion to dismiss.

Nevertheless, it bears emphasis that Wikimedia's core allegation—namely, that the NSA is copying and reviewing all the international text-based communications on the circuits it is monitoring—is not merely an allegation. The FISC has made clear that the NSA is searching the full text of every communication flowing through the surveillance devices installed on those international links. *See* [*Redacted*], 2011 WL 10945618, at *10, *15 (explaining that the NSA's Upstream surveillance devices search for and retain "*any* Internet transaction transiting the device if the transaction contains a targeted selector anywhere within it" (emphasis added)); *see also* PCLOB Report 122. This fact is presented, too, as textbook material in the leading treatise on national-security surveillance—one written, incidentally, by the former Assistant Attorney General

for National Security. *See* David Kris & J. Douglas Wilson, National Security Investigations and Prosecutions § 17.5 (2015) ("NSA's machines scan the contents of *all* of the communications passing through the collection point, and the presence of the selector or other signature that justifies the collection is not known until *after* the scanning is complete.") (emphasis in original). And it is described as fact by prominent members of the technology community. *See* Br. of Computer Scientists and Technologists 2-3, 8-15 ("[T]he NSA is copying and searching all communications that flow through the particular points on the internet 'backbone' at which the NSA has intervened.").[5]

Because the NSA searches *all* international communications that flow through certain circuits on the internet backbone, the government's argument that Wikimedia's trillion-plus communications may represent only a small portion of total internet traffic is beside the point. Def. Br. 37. Wikimedia's standing does not depend on its share of internet traffic. The crucial point is that Wikimedia's trillion-plus communications are sufficiently numerous and dispersed that they traverse each of the major internet circuits that carry traffic in and out of the country. Again, the government has *acknowledged* that it is monitoring some of those circuits. Pl. Br. 26-27. And the NSA's own documents confirm that

[5] *See id.* at 2 ("[I]t is certain, as a technical matter, that some of Plaintiff Wikimedia's communications have been subject to Upstream surveillance.").

Wikimedia's communications are among those that the government reviews and retains. *See* Compl. ¶ 107 (JA 63); Pl. Br. 33 n.12 (describing NSA computer code that allows analysts to identify intercepted Wikimedia communications).[6]

Finally, the government simply mischaracterizes how Upstream surveillance operates, calling it narrow and "targeted" when in fact it is broad and indiscriminate. Def. Br. 52 (quoting Op. at 20). In so doing, the government repeats one of the district court's basic misunderstandings of Upstream surveillance: that this surveillance is limited to the communications of legitimate foreign-intelligence targets. As Plaintiffs have explained, however, in order to identify communications to, from, and about its tens of thousands of targets, the NSA is first copying and reviewing *all* of the international text-based communications transiting the circuits it is monitoring. *See* Pl. Br. 27-33; Compl. ¶¶ 62-63 (JA 48-49). This surveillance is sweeping in its scope—and perhaps even unprecedentedly so:

> Nothing comparable is permitted as a legal matter or possible as a practical matter with respect to analogous but more traditional forms of communication. From a legal standpoint, under the Fourth Amendment the government may not, without a warrant, open and

[6] Despite the government's denials, Def. Br. 40, these documents show that the NSA is eager to acquire—and is in fact acquiring—communications between Wikimedia and the NSA's targets. The government contends that the documents offer no support because they do not expressly mention Upstream, but both pertain to an NSA search tool that allows analysts to retrieve and examine data intercepted in the course of Upstream surveillance as well as other programs. Compl. ¶ 107.

> read letters sent through the mail in order to acquire those that contain particular information. Likewise, the government cannot listen to telephone conversations, without probable cause about one of the callers or about the telephone, in order to keep recordings of those conversations that contain particular content.

PCLOB Report 122. Using surveillance devices installed on the internet backbone, the NSA is examining the contents of the communications of targets and non-targets alike.[7] In short, when the government calls the surveillance "targeted," it is referring to the *results* of its searches, while obscuring the fact that it searches the contents of countless other communications to find those of interest to it. It is akin to claiming that searching the contents of all letters passing through a mail processing center for thousands of names is "targeted," because only some of the letters mention those names. No court has ever embraced that false logic to find a search lawful, but regardless, it would be a question for the merits of this litigation, not a basis for denying standing.[8]

---

[7] *See* PCLOB Report 121-22 (describing surveillance of communications in which "the target is not a participant"); David Kris, *Trends and Predictions in Foreign Intelligence Surveillance*, 8 J. Nat'l Security L. & Pol'y 18 n.64 (2016), http://bit.ly/1WLjG8C (discussing Upstream surveillance and observing that it is unresolved whether the government should be permitted to "review the contents of an unlimited number of e-mails from unrelated parties in its effort to find information 'about' the target").

[8] The government also contends that Upstream surveillance is not "bulk" surveillance, but it is playing the same type of word game. Def. Br. 54 n.14. It emphasizes that it retains only some communications, but it ignores the fact that it searches all of them.

Wikimedia has plausibly alleged that its communications are subject to the surveillance it challenges. Wikimedia's detailed allegations do not remotely resemble the type of "bare assertion" that the Fourth Circuit has rejected as implausible under *Iqbal*. *See, e.g.*, *Johnson v. Am. Towers, LLC*, 781 F.3d 693, 709 (4th Cir. 2015); *Weidman v. Exxon Mobil Corp.*, 776 F.3d 214, 221 (4th Cir. 2015). Indeed, the government does not cite a single one of this Court's plausibility cases to support its position. That is not surprising; under the operative pleading standards, this case is not a close one. Wikimedia's well-pled allegations plausibly establish its standing.

C. Plaintiffs have plausibly alleged that the NSA is copying and reviewing "substantially all" international text-based communications, including their own.

As Plaintiffs explained in their opening brief, while Wikimedia would have standing even if the NSA were monitoring only a single major internet circuit, the NSA's surveillance activities are in fact much broader. *See* Pl. Br. 40-48. All of the Plaintiffs have standing to challenge Upstream surveillance because the NSA is copying and reviewing *substantially all* text-based communications originating or terminating in the United States, including the communications of Plaintiffs.

In response, the government once again disregards the presumptions that attach on a motion to dismiss. Like the district court, the government adopts a position directly at odds with the pleading rules, arguing—categorically—that

Plaintiffs "could not allege" sufficient facts to establish their standing because some facts about Upstream surveillance remain classified. Def. Br. 29 (quoting Op. at 18). That is wrong: the government's admissions are not the measure of plausibility. In any case, the existing public disclosures about Upstream surveillance establish Plaintiffs' standing. *Cf. ACLU v. Clapper*, 785 F.3d 787, 800-03 (2d Cir. 2015) (finding standing even while some aspects of the bulk call-records program remained classified).[9]

These public disclosures show that: (1) the government uses Upstream surveillance to "reliably" and "comprehensively" obtain communications to, from, and about its targets; (2) those targets number in the tens of thousands and are located all over the world; (3) the communications of these targets follow ever-changing paths across the internet; and (4) in order to conduct Upstream surveillance, the NSA has installed surveillance equipment at dozens of major chokepoints on the internet backbone. Pl. Br. 40-46. Together, these facts support Plaintiffs' allegation that the NSA is copying and reviewing substantially all international text-based communications. This allegation is consistent with the views of computer scientists, who have described the processes required to conduct

[9] Notably, the government has not invoked the state secrets privilege in this litigation. Indeed, in this context, the state secrets privilege has been preempted by statute. *See* 50 U.S.C. §§ 1806(f), 1881e(a) (preempting state secrets privilege where lawfulness of FISA and FAA surveillance is challenged).

Upstream surveillance. *See* Charlie Savage, *N.S.A. Said to Search Content of Messages to and from U.S.*, N.Y. Times, Aug. 8, 2013, http://nyti.ms/1E1nlsi (incorporated into complaint by reference, Compl. ¶ 69 (JA 51)).

Contrary to the government's argument, Plaintiffs' conclusion is not founded on a general assertion that the NSA has the capacity or motivation to collect intelligence. Def. Br. 29-33. It is founded, rather, on provable facts about the structure and operation of the internet. The surveillance could not operate as the government has described it except as Plaintiffs have alleged. This case is not like *Klayman v. Obama*, *see* Def. Br. 32, which came before the D.C. Circuit on the higher, preliminary-injunction standard and in which the plaintiffs put forward no evidence of the scale of the program beyond the government's desire to collect large amounts of call records. 800 F.3d 559 (D.C. Cir. 2015). Here, Plaintiffs not only allege the "who, what, when, and where" of the conduct they challenge, *SD3, L.L.C. v. Black & Decker, Inc.*, 801 F.3d 412, 430 (4th Cir. 2015), but also, significantly, *why* the surveillance operates as they describe.

The government is also wrong to fault Plaintiffs for relying on NSA documents and public reports that show the NSA is, in fact, conducting Upstream surveillance at dozens of backbone chokepoints operated by the largest telecommunications providers in the country. Pl. Br. 46 & n.16. The government argues, in effect, that Plaintiffs' allegations are implausible simply because these

documents do not use the word "most" or "all." Def. Br. 34 & n.11. But the documents and reports do not purport to be exhaustive. Rather, they confirm that—between just two of the participating providers—the NSA is monitoring at least 24 different backbone chokepoints. That is strong support for Plaintiffs' allegations about where and how the surveillance is being conducted.

Finally, contrary to the government's suggestion, Plaintiffs need not allege—let alone prove—that the NSA is copying and reviewing *every single* international internet communication at *every single* chokepoint. *See* Def. Br. 33-34. Rather, it is sufficient for Plaintiffs to allege that Upstream surveillance could not be implemented as the government has described it without examining substantially all internet traffic entering and leaving the country. *See Monsanto Co. v. Geertson Seed Farms*, 561 U.S. 139, 154-55 (2010) (finding Article III standing where party showed a "significant risk" that "gene flow" would affect plaintiff's crops); *Friends of the Earth v. Laidlaw Envtl. Servs. (TOC), Inc.*, 528 U.S. 167, 184-85 (2000) (finding standing where the "continuous and pervasive" discharge of pollutants into waterway affected plaintiffs' use of river and surrounding areas). That is precisely what Plaintiffs' allegations plausibly establish.

D. The government's declarations must be disregarded.

In addition to distorting the plausibility standard, the government impermissibly seeks to introduce its own declarations. However, because the

government brought a "facial" challenge to Plaintiffs' complaint—as opposed to a "factual" one—the government's two declarations are not properly before the Court, just as they were not properly before the district court. The law is clear: when assessing a facial challenge, a court cannot consider evidence beyond the complaint and documents incorporated by reference. Here, it is plain that the government's challenge was a facial one, and its belated protests to the contrary are belied by the record. Accordingly, this Court should disregard the government's declarations, as the district court concluded it was required to do. Op. at 10 n.8 (JA 183).[10]

The Fourth Circuit has explained that there are "two critically different ways" in which a defendant can move to dismiss for lack of subject-matter jurisdiction: it can contend that the complaint fails on its face to include allegations that would, if taken as true, establish subject-matter jurisdiction; or it can contend that the jurisdictional allegations of the complaint are not true as a matter of fact. *Adams v. Bain*, 697 F.2d 1213, 1219 (4th Cir. 1982); *Kerns v. United States*, 585 F.3d 187, 192-93 (4th Cir. 2009).

[10] If this Court concludes that the government presented a factual challenge below, it should remand the case so that Plaintiffs can put their own factual record—including expert testimony—before the district court. Moreover, for reasons discussed *infra*, that challenge must be resolved under Rule 56, not Rule 12(b)(1).

Despite what it now argues on appeal, in its motion to dismiss, the government brought only a facial—not factual—challenge. Its motion made no reference to a factual challenge, and it cited a single standard: *Iqbal's* plausibility standard. *See* Def. Mot. Dismiss 14, ECF No. 77-1 (contending that the Amended Complaint did not contain "sufficient factual matter, accepted as true" to "'state a claim [to standing] that is *plausible on its face*'" (quoting *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009)) (emphasis added)); *see also, e.g.*, *id.* at 3, 4, 13, 14, 16. Moreover, the government repeatedly relied on its declarations to argue that Plaintiffs' allegations were not "plausible," just as it does on appeal. *See* Def. Br. 39, 41, 43 ("Evidence submitted by the government confirms that plaintiffs failed to plausibly state an injury."). Because the government described its challenge solely as one to plausibility, the district court rightly held that the government's proffered declarations should be disregarded. Op. at 10 n.8 (JA 183).

Indeed, under this Court's precedents, the government *could not* permissibly have raised a factual challenge under Rule 12(b)(1), because here the jurisdictional question and merits questions are intertwined. *See Adams*, 697 F.2d at 1219; *Kerns*, 585 F.3d at 193 (intertwined factual issues must be resolved using the procedures "that would apply were the plaintiff facing a direct attack on the merits"). Plaintiffs' allegation that the government is unlawfully copying and reviewing their communications not only goes to Plaintiffs' standing, but it is also

one of the central elements of Plaintiffs' statutory and constitutional claims. Because this allegation is intertwined with the merits, any factual dispute over its truth would have to be resolved under Rule 56, not Rule 12(b)(1). *See Kerns*, 585 F.3d at 193.[11]

Finally, the government's contention that Plaintiffs forfeited their opportunity to rebut the government's factual claims is entirely without merit. Def. Br. 43. Plaintiffs made clear to the district court that they would submit their own evidence, including expert declarations, if the court construed the government's challenge as a factual one. Pl. Opp. to Mot. Dismiss 16 & n.11, ECF No. 86; *see Adams*, 697 F.2d at 1220 ("sufficient facts" must be developed before resolving a factual challenge). But the court correctly construed the government's challenge as a facial one.

The government is trying to have it both ways—that is, to have the benefit of its own facts without ever submitting to the *fact-finding* and discovery that would accompany a genuine factual contest. By casting its motion as a challenge to

[11] To permit a defendant to contest the truth of a plaintiff's injury-in-fact on a motion to dismiss—rather than as part of the merits of a claim—would significantly remake the course of civil proceedings. Cases permitting Rule 12(b)(1) factual challenges invariably involve *other* questions of personal or subject-matter jurisdiction, not challenges to a plaintiff's injury-in-fact, which is almost always intertwined with the merits. *Compare, e.g., United States ex rel. Vuyyuru v. Jadhav*, 555 F.3d 337, 347 (4th Cir. 2009), *with Potomac Conf. of Seventh-Day Adventists v. Takoma Acad. Alumni Ass'n*, 2 F. Supp. 3d 758, 767 (D. Md. 2014).

plausibility in the district court, the government sought to avoid any inquiry into whether it is in fact copying and reviewing Plaintiffs' communications. The declarations it submitted do not purport to address or resolve this question. Instead, those declarations—offered by two individuals with "no knowledge" of how Upstream operates, *see, e.g.*, Lee Decl. ¶ 13 n.5 (JA 107)—simply argue that the program does not "necessarily" function in the manner Plaintiffs allege. *See* Def. Mot. Dismiss 29-30. In other words, they are intended to make Plaintiffs' allegations appear less plausible.[12] The Court should reject the government's effort

[12] Significantly, neither Lee nor Salzberg claims to have any knowledge of how Upstream surveillance actually works. Instead, both provide misleading criticisms of Plaintiffs' allegations by offering opinions that fail to take into account the publicly disclosed facts. Lee, for instance, points out that physical submarine cables can contain multiple fibers, but he does not address how the internet *circuits* routed over these physical cables and fibers actually operate. Lee Decl. ¶¶ 11-13 (JA 106-07). As the government's disclosures make clear, Upstream surveillance is directed at major "circuits" or "links" on the internet backbone. PCLOB Report 36-37; [*Redacted*], 2011 WL 10945618, at *15; Compl. ¶¶ 60-61 (JA 47-48). Each of these circuits, which may span multiple fibers in a given cable, carries an enormous amount of international internet traffic from one provider to another. Because Lee does not address these circuits at all, he does not actually dispute the key allegation he purports to criticize. Moreover, Lee's assertions are at odds with the expert opinion of more than a dozen highly regarded computer scientists. *See* Br. of Computer Scientists and Technologists 2-3, 8-15.

The Salzberg Declaration is no more reliable. Plaintiffs' statistical illustration shows just how unlikely it is that Upstream surveillance does not touch *any* of Wikimedia's trillion-plus communications each year. Pl. Br. 35-37. Salzberg criticizes the illustration because it assumes that the surveillance is random. But as Plaintiffs explain, the properties that make Upstream surveillance non-random are properties that make it only *more likely* that Wikimedia is subject to this surveillance. For instance, Upstream is designed to capture precisely the type of

to prevail on plausibility by relying on one-sided, extrinsic evidence—evidence that the district court properly refused to consider.

II. *Amnesty* does not control this case because Plaintiffs do not challenge targeted surveillance.

The government erroneously argues that the standing inquiry in this case is controlled by *Amnesty*, in which the Supreme Court held that plaintiffs lacked standing because they could not prove that the surveillance they complained of was taking place, or that it ever would—let alone that their own communications would be subject to it. *See* Def. Br. 51. But where the *Amnesty* plaintiffs could only "speculat[e]" about the surveillance they challenged, 133 S. Ct. at 1148, here Plaintiffs have established—based on government disclosures and provable facts relating to the volume and dispersion of their own communications—that Upstream surveillance ensnares them.

First, the type of "speculation" that foreclosed the plaintiffs' standing in *Amnesty* is simply not at issue in this case. The *Amnesty* plaintiffs argued, but could not show to a sufficient likelihood, that the government was *targeting* communications to which the plaintiffs were party. *See id.* (discussing speculation concerning the government's decision to target, the government's choice of legal authority, FISC approval of that authority, the government's actual interception of

---

international text-based communications that Wikimedia engages in, while filtering out other types of communications. *See* Compl. ¶ 59 (JA 47).

targeted communications, and the plaintiffs' involvement in targeted communications). The thrust of the Court's analysis was that the plaintiffs could only speculate as to how government officials would exercise their discretion in choosing targets or legal authorities, and whether the FISC would actually authorize such surveillance. *Id.* at 1149, 1150 & n.5. Here, however, Plaintiffs have not challenged a hypothetical program of targeted surveillance, but rather a publicly acknowledged form of FISC-approved surveillance that involves the bulk copying and review of international communications. While not every operational detail of this surveillance is known, Plaintiffs have plausibly alleged—based on all that *is* known about Upstream surveillance—that it captures their communications.

Second, the government is wrong in arguing that "about" surveillance is "targeted insofar as it makes use of only those communications that contain information matching the tasked selectors." Def. Br. 52. As Plaintiffs have explained, in order to target communications containing selectors, the government must *first* copy and review essentially everyone's international communications. Pl. Br. 13-14. The government's argument entirely ignores the copying and review stages of Upstream surveillance—and thus ignores injuries that were not before the Court in *Amnesty*.

Finally, the government views *Amnesty* as an almost-categorical bar to standing, but even the five Justices in the majority were clear that different facts

could produce a different result. There is no question that this case presents such facts. For one thing, Wikimedia engages in so many internet communications that it is virtually unthinkable the government could avoid every single one of those communications while operating a surveillance program that systematically examines international internet traffic. Also, in *Amnesty* itself, the Supreme Court suggested that a lawyer who represented a target of FAA surveillance would have standing. *See* 133 S. Ct. at 1154. Plaintiffs' Amended Complaint identifies precisely such a lawyer. *See* Pl. Br. 55-57. Plaintiff NACDL's Joshua Dratel has taken costly and burdensome measures to protect the confidentiality of his communications, and as a result he has suffered an Article III injury traceable to Upstream surveillance.[13] A recently released FISC opinion only underscores the reasonableness of the measures he has taken. Mem. Op. at 50, *[Redacted]*, No. [Redacted] (FISC Nov. 6, 2015), http://1.usa.gov/1Vq8tLp (describing the FISC's "extreme[] concern[]" about the government's treatment of attorney-client communications). The facts alleged in this case go far beyond *Amnesty*, and it requires no "speculation" to conclude that Plaintiffs have adequately pled standing.

[13] The government says that Mr. Dratel cannot be certain whether the government is using Upstream or PRISM, but it is clear that the government uses *both* methods to surveil its individual targets. As the PCLOB Report emphasizes, the NSA uses Upstream to search for communications that it could not identify via PRISM. PCLOB Report 35, 119.

III. The government's copying and review of Plaintiffs' communications establish standing.

Though the district court did not reach the issue, the government argues that Plaintiffs lack standing even if it is true (as it is) that the NSA intercepts, copies, and reviews their communications. *See* Def. Br. 45-48. This argument fails for several reasons.

First, the government conflates the standing inquiry with the merits. The government is intercepting, copying, and reviewing Plaintiffs' communications, and so Plaintiffs are unquestionably entitled to invoke the Court's jurisdiction to test the legality of that surveillance. *See Clapper*, 785 F.3d at 801; *Amidax Trading Grp. v. S.W.I.F.T. SCRL*, 671 F.3d 140, 147 (2d Cir. 2011) (observing, in dicta, "[t]o establish an injury in fact—and thus, a personal stake in this litigation—[plaintiff] need only establish that its information was obtained by the government").

The government argues that Plaintiffs must further show that the interception, copying, and review of their communications invades interests protected by the Fourth Amendment, but this goes to the merits, not to standing. *Rakas v. Illinois*, 439 U.S. 128, 139-40 (1978) (stating that the definition of Fourth Amendment rights "is more properly placed within the purview of substantive Fourth Amendment law than within that of standing"); *Minnesota v. Carter*, 525 U.S. 83, 87 (1998) (criticizing courts for analyzing whether a party has "a

legitimate expectation of privacy" under "the rubric of 'standing' doctrine"); *United States v. Lawson*, 410 F.3d 735, 740 n.4 (D.C. Cir. 2005). In any event, it is well-settled that the interception of communications while in transit is not just an Article III injury, but a search or seizure within the meaning of the Fourth Amendment. That is true whether those communications are physical, *see Ex parte Jackson*, 96 U.S. 727, 733 (1877); *Hearst v. Black*, 87 F.2d 68, 70-71 (D.C. Cir. 1936) (government's copying of telegrams in transit was a "dragnet seizure" that violated sender's possessory and privacy rights), or electronic, *see Katz v. United States*, 389 U.S. 347, 353 (1967); *cf. LeClair v. Hart*, 800 F.2d 692, 695-96 & n.5 (7th Cir. 1986).

Second, even if Wikimedia had no cognizable privacy interest in its communications with its users, Wikimedia has separately alleged that Upstream surveillance invades its *possessory* and *expressive* interests in those communications. *See, e.g.*, Compl. ¶¶ 55, 73, 76, 89-95, 98-99, 113, 118, 131, 134 (JA 46, 52-53, 57-60, 66-68, 72-73) (describing Wikimedia's interest in controlling the information in its communications, including information in which Wikimedia has a protected associational interest). The government has never contested those well-pled allegations, and so, for the purposes of the standing inquiry, the question of whether Wikimedia has a protected *privacy* interest in its own communications is irrelevant.

The only question before the district court—and before this Court now—is whether Plaintiffs have plausibly alleged *standing*. This Court need not reach the merits in order to resolve the jurisdictional question, and the government's confused effort to conflate the two questions should be rejected. Because the government has engaged the merits, however, Plaintiffs feel obliged to address the merits briefly.

First, the government's novel legal theory notwithstanding, Def. Br. 47, 51, a computerized search is still a search. No case supports the government's radical "human eyes" theory of the Fourth Amendment. In fact, the only cases remotely on point make clear that the government cannot avoid the Fourth Amendment by carrying out privacy invasions using computers rather than human agents. *See, e.g.*, *United States v. Crist*, 627 F. Supp. 2d 575, 585 (M.D. Pa. 2008) (holding that using an electronic device to compare digital files on an individual's computer with other known files "constitutes a search").

Second, Wikimedia has asserted its own protected privacy interests—and not just those of its users—in its communications. The government's brief overlooks these extensive allegations. *Compare* Def. Br. 46, *with* Pl. Br. 16-18; Compl. ¶¶ 90-93, 95-96, 98-99, 102-04 (JA 57-62) (describing the different categories of Wikimedia communications and the range of sensitive and private information they contain). The government also overlooks the Supreme Court's

decision in *City of Los Angeles v. Patel*, which permitted motel operators to bring a Fourth Amendment challenge to the search of guest registries containing information about the motels' patrons. 135 S. Ct. 2443, 2447-48, 2452 (2015). Because Wikimedia's mission depends on the confidentiality of its communications, Compl. ¶¶ 98-99 (JA 59-60), Wikimedia's privacy interests in those communications are far stronger than the interests at issue in *Patel*.[14]

Third, the government is simply wrong that Wikimedia's communications disclose little about its users. Def. Br. 46. These communications reveal the IP addresses of Wikimedia's users, which are easy to link to particular individuals, revealing a great deal of sensitive information about what those users are reading and writing online. *See* Compl. ¶¶ 94-96 (JA 58-59); *see also* Dep't of Homeland Security, *Privacy Impact Assessment for the Use of Google Analytics* 2, 3, 11 (June 9, 2011), http://1.usa.gov/1yCTj4A (describing IP addresses as "personally identifiable information").

[14] The government cites no case for the proposition that organizations like Wikimedia lack a privacy interest in their own communications simply because they include information about individual patrons or customers, or because those communications are facilitated by computers. That is not surprising. Both the Wiretap Act and FISA recognize that companies have protected interests in their communications and authorize companies to sue for the unlawful interception of those communications. 18 U.S.C. §§ 2510(6), 2520 (permitting corporations to bring claims under the Wiretap Act); 50 U.S.C. §§ 1801 (i), 1810 (same under FISA). A ruling that companies lack a protected interest in their *own* communications, and thus lack standing to sue, would upend both these schemes.

Finally, Wikimedia has standing to assert the rights of its U.S.-person users. *See* Pl. Br. 61 (describing claims). Notably, in cases where the ability of individuals to speak, read, and write privately and anonymously is at stake—as it is here—the Supreme Court has been "quite forgiving" in applying its third-party standing test. *Kowalski v. Tesmer*, 543 U.S. 125, 130 (2004); *see Cooksey v. Futrell*, 721 F.3d 226, 234 (4th Cir. 2013). Regardless, Wikimedia has satisfied all three conditions for third-party standing: Wikimedia itself has stated an injury-in-fact based on the interception of its communications; Wikimedia enjoys an "active and close relationship" with many of the community members whose rights it seeks to protect, and thus it will be an effective proponent of its users' rights, Compl. ¶¶ 83-84, 101 (JA 54-55, 61); and Wikimedia's users face clear obstacles to litigating their own rights in this context. Indeed, users' interest in preserving their anonymity is precisely the kind of "practical obstacle" to bringing suit that gives rise to third-party standing. *Enterline v. Pocono Med. Ctr.*, 751 F. Supp. 2d 782, 786 (M.D. Pa. 2008).

IV. Plaintiffs' First Amendment injuries supply an independent basis for standing.

The government does not address Plaintiffs' First Amendment injuries except to say that "subjective 'chill'" is no basis for standing. Def. Br. 56. But the injuries to Plaintiffs' protected activities are objective and concrete. Wikimedia, for example, provides people around the world with access to free educational

content. Compl. ¶ 6 (JA 31). NSA surveillance, including Upstream surveillance, has caused a significant, sustained, and measurable decline in the number of readers accessing some of Wikimedia's resources. *See* Jonathon Penney, *Chilling Effects: Online Surveillance and Wikipedia Use*, 31 Berkeley Tech L.J. __ (forthcoming 2016). This drop-off in readers is a direct harm to Wikimedia itself, Compl. ¶ 110 (JA 64-65), and it is unlike any harm put before the Supreme Court in *Amnesty*. The government's "continuous and pervasive" monitoring of internet traffic is not hypothetical, and thus this injury is not a speculative or self-inflicted one. *Laidlaw*, 528 U.S. at 184-85. Wikimedia is akin to the world's largest library, and Upstream surveillance is driving away readers who would otherwise access this vast store of knowledge. This injury to First Amendment rights is sufficient in itself to support standing.

CONCLUSION

The district court's order dismissing Plaintiffs' Amended Complaint should be reversed.

May 6, 2016

Respectfully submitted,

/s/ *Patrick Toomey*

Deborah A. Jeon
David R. Rocah
AMERICAN CIVIL LIBERTIES UNION FOUNDATION OF MARYLAND
3600 Clipper Mill Rd., #350
Baltimore, MD 21211
Phone: (410) 889-8555
Fax: (410) 366-7838

Patrick Toomey
Jameel Jaffer
Alexander Abdo
Ashley Gorski
Brett Max Kaufman
AMERICAN CIVIL LIBERTIES UNION FOUNDATION

jeon@aclu-md.org

Charles S. Sims
David A. Munkittrick
PROSKAUER ROSE LLP
Eleven Times Square
New York, NY 10036
Phone: (212) 969-3000
Fax: (212) 969-2900
csims@proskauer.com

125 Broad Street, 18th Floor
New York, NY 10004
Phone: (212) 549-2500
Fax: (212) 549-2654
ptoomey@aclu.org

Counsel for Plaintiffs–Appellants

CERTIFICATE OF COMPLIANCE

1. This brief complies with the type-volume limitation of Fed. R. App. P. 32(a)(7)(B) because it contains 6,984 words, excluding the parts of the brief exempted by Fed. R. App. P. 32(a)(7)(B)(iii).

2. This brief complies with the typeface requirements of Fed. R. App. P. 32(a)(5) and the type-style requirements of Fed. R. App. P. 32(a)(6) because it has been prepared in a proportionally spaced typeface using Microsoft Word in 14-point Times New Roman.

/s/ Patrick Toomey
Patrick Toomey
Counsel for Plaintiffs–Appellants

Date: May 6, 2016

CERTIFICATE OF SERVICE

On May 6, 2016, I served upon the following counsel for Defendants–Appellees one copy of Plaintiffs–Appellants' REPLY BRIEF FOR PLAINTIFFS–APPELLANTS via this Court's electronic-filing system:

H. Thomas Byron, III
Catherine H. Dorsey
U.S. Department of Justice
950 Pennsylvania Avenue, NW
Washington, DC 20530
Phone: (202) 616-5367
H.Thomas.Byron@usdoj.gov

/s/ Patrick Toomey
Patrick Toomey
Counsel for Plaintiffs–Appellants

Date: May 6, 2016